KPMG

cutting through complexity™

Joint Internal Audit Protocol 2012/13

Dorset County Council
Dorset Fire
Dorset Police
West Dorset District Council
Weymouth and Portland Borough Council
Wiltshire Council

August 2012

AUDIT

Contents

This report is addressed to the Authorities and has been prepared for the sole use of the Authorities. We take no responsibility to any member of staff acting in their individual capacities, or to third parties. The Audit Commission has issued a document entitled *Statement of Responsibilities of Auditors and Audited Bodies*. This summarises where the responsibilities of auditors begin and end and what is expected from the audited body. We draw your attention to this document which is available on the Audit Commission's website at www.auditcommission.gov.uk.

External auditors do not act as a substitute for the audited body's own responsibility for putting in place proper arrangements to ensure that public business is conducted in accordance with the law and proper standards, and that public money is safeguarded and properly accounted for, and used economically, efficiently and effectively.

If you have any concerns or are dissatisfied with any part of KPMG's work, in the first instance you should contact Harry Mears or Chris Wilson, the appointed engagement leads to the Authorities, who will try to resolve your complaint. If you are dissatisfied with your response please contact Trevor Rees on 0161 246 4000, or by email to trevor.rees@kpmg.co.uk, who is the national contact partner for all of KPMG's work with the Audit Commission. After this, if you are still dissatisfied with how your complaint has been handled you can access the Audit Commission's complaints procedure. Put your complaint in writing to the Complaints Unit Manager, Audit Commission, Westward House, Lime Kiln Close, Stoke Gifford, Bristol, BS34 8SR or by email to complaints@audit-commission.gov.uk. Their telephone number is 0844 798 3131, textphone (minicom) 020 7630 0421.

Engagement Team

The contacts at KPMG in connection with this protocol are detailed here:

Key Contact Name	Contact Details	Authority
Chris Wilson	*Partner, KPMG LLP (UK)* Tel: 011 89642238 christopher.wilson@kpmg.co.uk	Wiltshire Council
Harry Mears	*Associate Partner, KPMG LLP (UK)* Tel: 023 80202093 harry.mears@kpmg.co.uk	Dorset County Council Dorset Fire Authority Dorset Police Authority West Dorset District Council Weymouth & Portland Borough Council
Darren Gilbert	*Senior Manager, KPMG LLP (UK)* Tel: 029 2046 8205 darren.gilbert@kpmg.co.uk	Dorset County Council Wiltshire Council
Claire Hollick	*Senior Manager, KPMG LLP (UK)* Tel: 023 80206000 claire.hollick@kpmg.co.uk	Dorset Fire Authority Dorset Police Authority West Dorset District Council Weymouth & Portland Borough Council
John Oldroyd	*Manager, KPMG LLP (UK)* Tel: 023 80202055 john.oldroyd@kpmg.co.uk	Dorset County Council
Alex McCabe	*Assistant Manager, KPMG LLP (UK)* Tel: 023 80202026 alexander.mccabe@kpmg.co.uk	Dorset County Council Dorset Fire Authority Dorset Police Authority
Rob Laidler	*IT Manager, KPMG LLP (UK)* Tel: 011 79054251 robert.laidler@kpmg.co.uk	Dorset County Council Wiltshire Council

Introduction

This document sets out KPMG's approach to the audit of key controls in place at Dorset County Council, Dorset Fire, Dorset Police, West Dorset District Council Weymouth and Portland Borough Council and Wiltshire Council ("the audited bodies").

Purpose and structure of this document

Auditing standards and KPMG policy in the UK prohibit auditors from seeking direct assistance from Internal Audit. We are, however, permitted to review any audit work that may have been carried out with a view to potentially placing reliance on this work, to support our work in relation to the audited bodies' financial statements. We therefore use joint working agreements, such as this document, to share information on possible testing that Internal Audit may choose to undertake, which would facilitate our ability to rely upon it.

This document identifies those key areas where KPMG may seek to rely on the controls operated by management over its financial systems.

The aim of this document is to link together all the mutual clients of KPMG and South West Audit Partnership (SWAP) and to produce one common working protocol between internal and external audit to enable efficiencies of working together.

Key Contacts

For the purposes of reviewing any work undertaken by Internal Audit or for regular discussion of their findings, our main contact within SWAP is Dave Hill (email: Dave.Hill@southwestaudit.gov.uk).

Suggested actions

This document is addressed to the audited bodies' management who may wish to share it with their Internal Auditors. Where the testing detailed in this document is undertaken by Internal Audit, we may seek to rely on this work in order to avoid duplication of work and increased costs to the audited bodies.

We have included in Appendix A a list of the controls we would expect to rely on in relation to our audit of the financial statements, and our testing requirements in relation to these. Internal Audit should confirm to us where their work will incorporate the testing specified.

Scope and responsibilities

The main areas where KPMG seeks to rely on work performed by Internal Audit centres on our responsibility as external auditors to give an independent assessment of:

- Whether the statements of accounts fairly present the financial position of the audited bodies and their income and expenditure accounts and balance sheets for the year in question, have been properly prepared in accordance with the appropriate legislation; and
- The adequacy of the audited bodies' arrangements for ensuring the economic, efficient and effective use of resources.

In completing this role we will have regard to both the adequacy of the audited bodies' financial systems and the adequacy of their arrangements for preventing and detecting fraud and corruption.

Internal Audit support these responsibilities primarily through cyclical reviews of systems. The following additional responsibilities also indirectly contribute:

- Ad hoc investigations into suspected fraud or corruption;
- Input to systems development and replacement; and
- Advising the audited bodies on the implementation of national initiatives.

Working together

In order to ensure that an effective working relationship is maintained, KPMG will, with Internal Audit:

- Discuss the risk assessment underlying our respective audit plans, to determine who is best placed to audit areas of common interest;
- Share terms of reference and final reports for specific reviews, including those performed by specialists (e.g. IT reviews);
- Share details of specific review kick-off meetings and debriefs, to give teams the opportunity to attend meetings; and
- Attend meetings of the Audit Committee, where necessary for our reports to be presented.

Where we have identified the opportunity to rely on work performed by Internal Audit, we will consider the findings of their report and review the supporting audit files. Auditing standards also require that we re-perform an element of Internal Audit's work, in order to place reliance on it.

General arrangements

Planning and liaison

Internal Audit's operational plan is fine-tuned, taking into account any carried forward risk from the previous year and/or local developments, on an annual basis. We will review the strategic and annual planning processes as part of our overall procedures for assessing the adequacy of internal audit arrangements (see 'Internal Audit effectiveness' below).

Regular liaison between the Head of Internal Audit and the KPMG Audit Managers will take place, typically through meetings. Standard agenda items are likely to include:

- Update against Internal Audit's and KPMG's audit plans.
- Confirmation of reports finalised.
- Confirmation of fraud flashes and warning bulletins issued and resulting "hits".
- Significant concerns about financial systems or the financial performance of the client.
- Details of special investigations.
- Other issues, for example Internal Audit involvement in system development work or new requirements from the Audit Commission

KPMG and Internal Audit will distribute finalised reports to each other, after the agreement of the findings with the audited bodies.

Internal Audit effectiveness

On a cyclical basis, and as a precursor to reliance on Internal Audit's work, KPMG will perform an overall management arrangements review of the Internal Audit function. The scope of this review will be shared with Internal Audit as part of this process. On an annual basis, through our audit approach we are required to form a judgement on the adequacy of the internal audit functions. Specifically we are required to review the risk based internal audit plan to ensure that Internal Audit have reviewed all high risk financial systems on an annual basis and medium risk financial systems on a cyclical basis.

The findings arising from the review will be sent in draft to the Head of Internal Audit and the action plan discussed before it is shared with the audited bodies.

Review of IA working papers

Where KPMG intend to place reliance on Internal Audit work we will undertake a detailed review of their working papers. This encompasses the scope of work, sample sizes, audit evidence and review procedures. Work may be reviewed and reliance planned when work is not quite complete (for example, testing not complete, file not reviewed), however, KPMG will revisit the work to check appropriate completion later in the audit year.

The review of files will be arranged at a mutually convenient time and place. We would envisage this during our interim (financial systems) audit, which would typically take place between February and April of each financial year. KPMG will also re-perform Internal Audit's testing on a sample basis. Should the results of the review reveal particular strengths or weaknesses in the audit process these will be discussed with the Head of Internal Audit as soon as possible.

External Audit responsibilities

Under the Audit Commission's Code of Audit Practice external auditors are required to provide assurance that financial statements are: "*…. free from material misstatement, whether caused by fraud or other irregularity or error;… comply with statutory and other applicable requirements…and comply with all relevant requirements for accounting presentation and disclosure*"

In addition, part of KPMG's approach is to work to understand the events, transactions and practices that, in our judgement, may have a significant effect on the financial statements, supporting our accounts objective. At our interim audit this involves using our knowledge of the financial systems to identify and test the overall high-level controls, for example reconciliations, which provide assurance over the figures used to prepare the accounts. This work will draw on that of Internal Audit where possible.

Consideration of Fraud Risk

As part of our audit we assess the risk of fraud in accordance with the revised International Standard on Auditing 240, *The Auditor's Responsibility to Consider Fraud in an Audit of Financial Statements* (revised ISA 240). We consider this standard to be a key component in ensuring the quality of audits, which is the cornerstone of our audit practice. Part of this process is to pragmatically and realistically consider fraud risk factors and plan our audit accordingly. We complete this through the incorporation and consideration of fraud risk concerns within our Fraud Audit Program. This provides our team with a step-by-step approach in their consideration of risk of material misstatement due to fraud in each phase of the audit process and addresses relevant documentation requirements.

The role of internal auditors is to ensure that a risk based approach is adopted to the audit of the audited bodies' systems of internal financial control. Additionally, Internal Audit should ensure that it performs its work while paying due regard to the risk of fraud and corruption as part of its risk based approach.

In addition, information in this area is required to flow both to and from the Audit Commission, in particular:

- *Flow of information to the Audit Commission* - auditors are required to return AF70 forms to the Audit Commission for any proven fraud with a value in excess of £10,000. We would ask that Internal Audit in their capacity take responsibility for completion of these forms as part of the routine investigation of cases of fraud.
- *Flow of information from the Audit* Commission – from time to time the Audit Commission publishes warning bulletins and fraud flashes. These will be passed to Internal Audit promptly for action. Internal Audit will inform KPMG of any "hits" and the subsequent action taken.

To ensure that there is on-going liaison Internal Audit will inform KPMG of all investigations as soon as possible. Where directed by management, Internal Audit will also assist in ensuring that appropriate action is taken in response to the National Fraud Initiative (NFI) that is currently performed every two years by the Audit Commission.

Minimum sample sizes

KPMG's approach to testing significant financial systems ensures that we test samples taken throughout the financial year, although these do not need to cover the entire financial year (for example, alternate months across the year). For clarity, those controls upon which KPMG aim to rely on an annual basis for each Authority are set out in *Appendix A*. To ensure that we obtain sufficient assurance over the operation of these controls our samples (and therefore those of internal audit work on which we are to rely) must meet the certain minimum sample size criteria.

The extent of testing also depends on the risk of failure of the control being tested, which is the risk that the control might fail and, if it failed, that a material misstatement in the financial statements would result. We consider the following factors when assessing the risk of failure associated with a control:

- the nature and materiality of the misstatements which the control is designed to prevent or detect;
- the inherent risk associated with the relevant significant account and assertions;
- whether there have been changes in the volume or nature of transactions over which the control operates;
- the competence of the personnel who perform the control or monitor its performance, and whether there have been changes in such personnel;
- the complexity of the control and the significance of the judgments that must be made in connection with its operation; and
- whether the significant account has a history of errors.

Audit of the financial statements

This page reflects the minimum levels of the sample sizes for testing of the controls, presented in Appendix A.

Our audit work is completed in accordance with the KPMG Audit Manual (KAM). The KAM sets out standards to which we must adhere in our audit work. Similarly, if we are seeking to rely on the work of internal auditors, their testing would need to meet KAM requirements to avoid the need for us to carry out extra work.

In order to place reliance on this work, we expect working papers to demonstrate that:

- An appropriate sample size has been used;
- The sample has been appropriately selected – for example, details of where the sample was chosen from and how it was selected being set out on the working paper; and
- The testing covers the whole financial year, or year to date.
- The required work should include walkthroughs (testing of a single case to verify the documentation of systems and controls), testing of design, implementation and operation of controls.

It is important to apply a flexible approach to sample testing, for example:

- **If the expected control set out in this protocol does not operate in the Council (for example because of the way in which a system is configured), then it is important to consider whether there are alternative or compensating controls which exist that meet the objective and, if so, test these instead**; and
- **If sample testing identifies any errors** (for example, the inconsistent application of a control or lack of documentation that the control has operated) then it is **important for the auditor to consider whether additional sample testing is necessary, or if there are compensating controls which may provide the required assurance**, before concluding on the operating effectiveness of that control (the results of the original sample testing should of course be documented and reported appropriately).

It should be noted that our review of these controls considers the effectiveness of their design, their implementation and their effective operation. We are required by auditing standards to perform 'walkthroughs' of controls within a system to confirm that the controls are being implemented in a way consistent with our understanding. In order for us to rely on walkthroughs conducted by Internal Audit, these must document all relevant information, including transaction references at each stage of the process.

Frequency of control activity	Risk of Control is Lower The minimum sample size is:	Risk of failure of Control is Higher The minimum sample size is:
Quarterly	2 transactions or events (including period end)	2 transactions or events (including period end)
Monthly	2 transactions or events	3 transactions or events
Weekly	5 transactions or events	8 transactions or events
Daily	15 transactions or events	25 transactions or events
More than daily	25 transactions or events	40 transactions or events

Audit of the financial statements

We expect Internal Audit working papers to enable us to clearly identify the relevant factors for each area reviewed.

The KAM methodology aims to secure compliance with International Standards on Auditing (UK and Ireland) (ISAs). One key standard is ISA230 *Audit Documentation*.

We expect that the Internal Audit work we rely on enables us to meet the requirements of imposed by the ISA. In order to ensure compliance, we expect Internal Audit working papers to enable us to clearly identify the following factors for each area reviewed:

- Nature, timing and extent of audit procedures performed;
- Results of procedures and evidence obtained; and
- Significant matters arising, and conclusions reached.

We therefore expect the information contained within the audit files to detail the following for each high level control reviewed:

Feature of audit documentation	Purpose
Documentation of the identifying characteristics of specific items or matters being tested	Recording the identifying characteristics serves a number of purposes. It enables the audit team to be accountable for its work and facilitates the investigation of exceptions or inconsistencies. Identifying characteristics will vary with the nature of the audit procedure and the item being tested, for example: • For a detailed test of purchase orders, the auditor may identify the documents for testing by their dates and unique purchase numbers; • For a procedure requiring selection or review of all items over a specific amount from a population, the scope of the procedures, and population may be identified (for example, all journal entries over a specified amount from the journal register).
Significant matters	Judging the significance of a matter requires an objective analysis of the facts and circumstances. These may include: • Matters that give rise to significant risk; • Results of audit procedures indicating that financial information could be materially misstated; • Circumstances which cause the auditor significant difficulty in applying necessary audit procedures; and • Findings which could result in a modification to the auditor's report (or, in the case of Internal Audit, this might be a significant matter which could lead to a "no assurance" opinion for the review). Discussions of a significant matter with officers should be documented on a timely basis.
Identification of Preparer and Reviewer	In documenting the nature, timing and extent of audit procedures performed, the auditor should record: • Who performed the audit work, and the date such work was completed; and • Who reviewed the audit work performed, and the date and extent of such review.

Summary of controls to be tested

This appendix records the key controls that KPMG seek to test on an annual basis, to support our opinion on the accounts. Sample sizes for testing of controls should meet or exceed the minimum levels on page 6.

Key:

Blue: All Authorities

Green: DCC only

Orange: West Dorset, Weymouth and Portland and Wiltshire Council only.

Purple: Wiltshire Council only.

Grey: DCC and WC only.

Control	Specific area of testing	Detailed testing requirements
Debtors		
Periodic reconciliations of the general ledger to all material debtors codes/systems	Discuss with management the process for the reconciliation and review between the income/sundry debtors system and the general ledger, using one reconciliation as an example, showing how it is performed and any follow up of reconciling items.	For a sample in line with the sample size set out on page 6, confirm that reconciliations have been produced on a timely basis and evidenced as reviewed.
		Confirm that balances can be supported, no material reconciling items exist and the reconciliation casts.
Periodic reconciliation of the debtors system to the cash receipting system.	Discuss with management the process for the reconciliation and review between the debtors system and the cash receipting system, using one reconciliation as an example, obtaining explanations for any significant reconciling items.	For a sample in line with the sample size set out on page 6, confirm that reconciliations have been produced on a timely basis and evidenced as reviewed.
		Confirm that balances can be supported, no material reconciling items exist and the reconciliation casts.
Periodic production and independent review of sundry debtors arrears reports.	Review a sample of debtors arrears reports in line with sample sizes as set out on page 5, from the audited year to ensure that they are produced and independently reviewed with the frequency prescribed by the Authority's financial procedures.	Select a sample of debtors that are of an age such that recovery action should have been instituted and confirm with management the action being taken to recover them. Review the process and obtain supporting documentation, such as email trails, to confirm this process is being followed.
	Ensure that there are appropriate authorisation levels in place for the write-off of debtors. Discuss how this is distributed to staff.	Confirm that the write-off of debtors has been undertaken on a regular basis in line with the audited bodies' SFIs and SOs.
		Select a sample of write-offs across each service area and confirm that the appropriate authorisation has been obtained.
Monthly monitoring of income against budget.	Discuss with management the process for reviewing budgetary control information produced to ensure that income variances against budget are identified, reported and robustly investigated. Use one month as an example to follow the process through, ensuring that it has been performed and reviewed in line with management's assertions.	For a sample in line with the sample size set out on page 6, check that the reports were produced each month, and that information contained is consistent with the general ledger.
		For sampled months, identify all material variances and obtain evidence from management accountants to confirm that the variance has been robustly investigated and explanations documented.
Walkthroughs: Setting up a new account; Invoice raising and dispatch; Cash receipting; Arrears Recovery; Debtors system updating of the general ledger.		

Summary of controls to be tested (continued)

Control	Specific area of testing	Detailed testing requirements
Non pay expenditure and creditors		
Periodic reconciliation of the creditors system to the general ledger.	Discuss with management the process for the reconciliation between the creditors system and the general ledger, agreeing significant reconciling items to source systems or other supporting documentation. Use one reconciliation as an example to walk through.	For a sample in line with the sample size set out on page 6, confirm that reconciliations have been produced on a timely basis and evidenced as reviewed.
		Confirm that balances can be supported, no material reconciling items exist and the reconciliation casts.
Implementation of procurement policy	Discuss with management the process for new contracts/supplier arrangements. Obtain the official documentation disseminated to staff detailing the process. For one purchase ensure it is followed.	For a sample in line with the sample size set out on page 6, Confirm that the authority has complied with the procurement policy for a sample of new contracts (eg where OJEU notices may be required, range of tenders obtained, checks on new suppliers)
Authorisation of purchase invoices and matching against PO and GRN.	Discuss with management how trade and non trade purchase invoices are authorised and matched against PO and GRN. Walk through one purchase invoice paid in year to ensure this process is followed.	For a sample in line with the sample size set out on page 6, ensure authorisation for purchase invoices is obtained from an appropriate person and within their authority limit. Ensure that it has been matched to a PO and GRN as appropriate.
Independent review of exceptions – e.g. payments to new suppliers, potentially duplicated payments, payments over a certain size	Discuss with management the process for production and review of any exception reports, frequency of reports and what they cover. Review one report which has been produced and ensure it is consistent with management's assertion.	For a sample in line with the sample size set out on page 6, ensure that payments requiring exception review, have had formal sign off.
		Scan review payment records and document frequency of payment made that would require exception review.
Monthly monitoring of non-pay expenditure against budget.	Discuss with management the process for reviewing budgetary control information to ensure that non pay expenditure variances against budget are identified, reported and robustly investigated. Use one month as an example to follow the process through, ensuring that it has been performed and reviewed in line with management's assertions.	For a sample in line with the sample size set out on page 6, check that the reports were produced each month, and that information contained is consistent with the general ledger.
		For sampled months, identify all material variances and obtain evidence from management accountants to confirm that the variance has been robustly investigated and explanations documented.
Walkthroughs: Setting up a new supplier; Raising orders; Receipting Goods; Invoice processing (including 3 way match of order, goods received note and invoice); Creditors system update to general ledger.		

Summary of controls to be tested (continued)

Control	Specific area of testing	Detailed testing requirements
Housing and Council Tax Benefits – WDDC, WPBC and WC only		
Periodic reconciliation of Council Tax system to the Benefits system.	Discuss with management the process for the reconciliation of all benefits between the Council tax system and the benefits system, obtaining explanations for significant reconciling items. For one month review the reconciliation performed and ensure it is performed and reviewed in line with management's assertions.	For a sample in line with the sample size set out on page 6, confirm that reconciliations have been produced on a timely basis and evidenced as reviewed. Confirm that balances can be supported, no material reconciling items exist and the reconciliation casts.
Periodic reconciliation of the Housing Benefit system to the general ledger.	Discuss with management the process for the reconciliation. For one reconciliation ensure that it has been performed and reviewed in line with management's assertions. Obtain explanations for significant reconciling items.	For a sample in line with the sample size set out on page 6, confirm that reconciliations have been produced on a timely basis and evidenced as reviewed. Confirm that balances can be supported, no material reconciling items exist and the reconciliation cast.
Periodic reconciliation of the Council Tax Benefits per the Council Tax system to the general ledger.	Discuss with management the process for the reconciliation of all benefits between the benefits system and the general ledger. For one reconciliation ensure that it has been performed and reviewed in line with management's assertions, obtaining explanations for significant reconciling items.	For a sample in line with the sample size set out on page 6, confirm that reconciliations have been produced on a timely basis and evidenced as reviewed. Confirm that balances can be supported, no material reconciling items exist and the reconciliation casts,.
Exception reporting (e.g. to identify un-presented cheques)	Discuss the requirement for any exception reports which are produced and the frequency of production with management. Discuss the process for review and authorisation. For one report ensure that this has been performed in line with management's assertions.	For a sample of payment reports requiring exception reports, as per the sample sizes on page 6, confirm that formal sign off of the review exists. Scan review payment records and document frequency of payment made that would require exception review.
Walkthroughs: Will be performed as part of the HBCTB grant claim audit performed by KPMG.		

Summary of controls to be tested (continued)

Control	Specific area of testing	Detailed testing requirements
Housing Rent –WC only		
Periodic reconciliation of the rents system to the cash receipting system	Discuss the reconciliation process with management, ensuring it picks up all incoming rents. Assess whether the reconciliation, follow up of reconciling items and review are appropriate and timely. For one reconciliation ensure it has been performed in accordance with management's assertions.	For a sample in line with the sample sizes on page 6, confirm that reconciliations have been produced in a timely fashion and have been evidenced as prepared and reviewed. Confirm that the reconciliation casts and agree systems balances and significant reconciling items to supporting documentation.
Periodic reconciliation of the rents system to the general ledger	Discuss the reconciliation process with management, ensuring it picks up all rents. Assess whether the reconciliation, follow up of reconciling items and review are appropriate and timely. For one reconciliation ensure it has been performed in accordance with management's assertions.	For a sample in line with the sample sizes on page 6, confirm that reconciliations have been produced in a timely fashion and have been evidenced as prepared and reviewed. Confirm that the reconciliation casts and agree systems balances and significant reconciling items to supporting documentation.
Periodic review and reporting of arrears levels and rent accounts in credit	Ensure that arrears reports are produced routinely Confirm whether the control is designed in such a way that it would prevent and detect material misstatement or fraud.	For a sample in line with the sample sizes on page 6, ensure arrears reports and accounts in credit have been independently reviewed throughout the year with appropriate action taken.
Walkthroughs:		

Summary of controls to be tested (continued)

Control	Specific area of testing	Detailed testing requirements
School Information Management Systems (SIMS) –DCC and WC		
Periodic reconciliation of the SIMS system to the general ledger	Discuss the reconciliation process with management. Assess whether the reconciliation, follow up of reconciling items and review are appropriate and timely. For one reconciliation ensure it has been performed in accordance with management's assertions.	For a sample of reconciliations in line with the sample sizes on page 6, confirm that reconciliations have been produced in a timely fashion and have been evidenced as prepared and reviewed. Confirm that the reconciliation casts and agree systems balances and significant reconciling items to supporting documentation.
Production and review of exception reports (e.g. to identify individual items of significant expenditure)	Discuss the exception report process with management, ensuring it picks up all relevant, potential exceptions. Assess whether the follow up and investigation of exceptional items and review are appropriate and timely. For one report ensure it has been reviewed in accordance with management's assertions.	For a sample of payments, in line with the sample sizes on page 6, highlighted by the exception report, confirm that these agree to supporting documentation
Reconciliation of schools bank balances	Discuss the process for reconciliations with management, including the process for investigating reconciling items and review. For one reconciliation ensure that this process has been followed.	For a sample in line with the sample sizes on page 6, confirm that reconciliations have been performed on a timely basis and evidenced as reviewed. Agree systems balances and significant reconciling items to supporting documentation. Ensure all bank accounts with a significant balance and all frequently used bank accounts are considered.
Walkthroughs: None		

Summary of controls to be tested (continued)

Control	Specific area of testing	Detailed testing requirements
Payroll and pensions/IAS 19		
Periodic reconciliation of the payroll system to the general ledger.	Discuss with management the frequency of reconciliation between the payroll system and general ledger. For one reconciliation ensure it has taken place and reconciling items have been appropriately followed up and that the reconciliation is evidenced as reviewed.	For a sample in line with the sample sizes on page 6, confirm that reconciliations have been produced on a timely basis and evidenced as reviewed. Confirm that balances can be supported, no material reconciling items exist and the reconciliation casts.
Periodic reconciliation of the payroll system to personnel records.	Ensure that personnel and payroll records are reconciled periodically with respect to: • numbers of staff • hours/WTE basis of staff • pay grades of staff	For a sample in line with the sample sizes on page 6, confirm that reconciliations have been produced on a timely basis and evidenced as reviewed. Re-perform the year end reconciliation, and one further reconciliation from the audited year to ensure that it was appropriately completed.
Either:		
Authorisation of starters and leavers.	Discuss with management the formal process for authorising new starters and what is required before they can start work, eg signed contract, right to work in UK etc. For leavers discuss the process for notification to HR and payroll. For one starter per the payroll system and one leaver per HR, ensure this process has been followed appropriately.	For a sample of joiners in line with the sample sizes on page 6, obtain signed copy of starters form , right to work in UK and signed contract and ensure that individual is added to the payroll in a timely fashion. For leavers agree the individuals leaving date to their leavers form and ensure that the individual is removed from the payroll in a timely manner.
Or:		
Periodic circularisation of establishment lists to Chief Officers / Budget Holders	Discuss with management whether establishment lists are been circularised to Chief Officers / Budget Holders on a monthly basis and discuss the process for review and investigation of any variances.	Review a sample of months, in line with the sample sizes on page 6, to ensure that positive confirmation of employee validity was received in all cases, and that action was taken to resolve issues.
Production and independent review of exception reports –e.g. movement in individual net pay >10% (not practical for DCC due to size of report)	Discuss what exception reports are produced with management, the process for investigating the exceptions and the review process. For one report ensure this process has been followed.	For a sample of exception reports as per the sample sizes on page 6, confirm that formal sign off of the review exists and that exceptional items have been appropriately investigated.
Management review of BACS payment run	Discuss with management how the payroll BACS runs are authorised. For one run ensure this process has been followed.	For a sample of BACS payment runs as per the sample sizes on page 6, ensure appropriate authorisation took place.

Appendix A

Summary of controls to be tested (continued)

Control	Specific area of testing	Detailed testing requirements
Pension Fund audits – DCC and WC		
Authorisation of benefit payments to include lump sums on death, lump sums on retirement and transfer out payments.	Discuss the review and authorisation process for calculations of benefits on death, retirees and transfers out.	For a sample of lump sums on death, retirement and transfers out obtain copies of signed leaver forms and benefit calculations. Ensure that the benefit calculation and subsequent payment has been reviewed and authorised. For death benefits ensure that there is a death certificate on file.
Production and independent review of exception reports produced for pension payroll	Discuss the process for the production and review of exception reports. Ensure this is appropriate and for one report ensure this has been performed in line with our understanding.	For a sample of payments highlighted by the exception report, confirm that there is evidence of investigation and formal sign off of the review.
Authorisation of starters and leavers to the pension payroll	Discuss the process for adding and removing employees from the pension scheme. Ensure that this is appropriate. For one starter per the system, and one leaver per HR, ensure that the process has been performed appropriately and in a timely manner.	For a sample in line with the sizes on page 6, obtain signed copy of starters form and ensure that individual is added to the payroll accurately and in a timely fashion in accordance with the pension calculation. For a sample of leavers in line with the sizes on page 6, agree the individuals leaving date to their leavers form and death certificate. Ensure that the individual is removed from the payroll in a timely manner.
Periodic reconciliation of the pension payroll system to the general ledger	Discuss the reconciliation and review process with management. Ensure it is appropriate and done in a timely manner. For one reconciliation ensure that it has been performed and reconciling items appropriately followed up.	Confirm that reconciliations have been produced in a timely fashion and have been evidenced as prepared and reviewed. Confirm that the reconciliation casts and any material reconciling items exist and agree to supporting documentation.
Bank reconciliations	Discuss the reconciliation and review process with management. Ensure it is appropriate and done in a timely manner. For one reconciliation ensure that it has been performed and reconciling items appropriately followed up.	Confirm that reconciliations have been produced in a timely fashion and have been evidenced as prepared and reviewed. Confirm that the reconciliation casts and agree systems balances and significant reconciling items to supporting documentation.

Summary of controls to be tested (continued)

Control	Specific area of testing	Detailed testing requirements
Pension fund audits – DCC and WC		
Evidence of regular discussions with Governors and the actuary on the pension deficit. (relates to DCC and WC only)	Ensure that discussions regarding the pension deficit have taken place during the year.	Obtain copies of any meeting minutes or notes available to confirm that appropriate discussions have taken place.
Management approval of IAS 19 assumptions. (relates to DCC and WC only)	Ensure that the assumptions used by the actuary in the IAS 19 valuation have been reviewed and approved by management.	Confirm that management have reviewed and approved the IAS 19 assumptions through enquiry, and observation of any supporting documentation. Eg. formal sign off.
Walkthroughs: New Starters; Permanent amendments; Temporary amendments; Leavers; Payroll payment runs; Processing of payroll transactions into the general ledger.		
Capital accounting and asset management (DCC)		
Five-year rolling programme of revaluation for fixed assets held at current cost	Ensure that the Authority has complied with its revaluation programme in the year and that all assets accounted for on a current value basis have been re-valued within the last five years.	Obtain from the asset register a report detailing all assets revalued in the year to date. Confirm that entries reconcile back to the list of assets scheduled for revaluation in year and any disposals undertaken.
		Confirm the five largest revaluations back to third party supporting evidence provided by the valuer.
		Ensure that all assets have had a professional valuation prior to disposal.
Annual impairment review of tangible and intangible fixed assets	Obtain a list of officers responsible for assessing whether impairment review of assets is necessary.	Consider the findings of the Authority's impairment review.
		Ensure that both types of impairment (market value or consumption of economic benefits) have been considered and that the Authority has made an impairment with the appropriate accounting treatment where the need for an impairment is identified.
		Confirm for a sample of 5 impairments and 5 other changes identified as part of the control process that the fixed asset register has been updated as required.

Summary of controls to be tested (continued)

Control	Specific area of testing	Detailed testing requirements
Periodic reconciliation of the fixed asset register to the general ledger	Obtain a listing of all the general ledger codes used to record fixed asset expenditure and annotate this to show what reconciliation is performed to confirm the accuracy of each code	Review the year end reconciliation (and one further reconciliation from the audited year if the reconciliation is more than annual) between the fixed asset register and the general ledger, agreeing significant balances to supporting documentation. Consider comparing the asset register to other records –e.g. Asset Management Plan.
Review of capital expenditure against the capital programme	Discuss with management how often the expenditure against the programme is monitored and how variances against expectations investigated and documented. For one review ensure this has been appropriately performed.	For a sample in line with that on page 6, confirm that capital expenditure information used is consistent with the general ledger.
		Obtain an explanation for any material variances against the capital programme in those reconciliations.
Periodic physical verification of tangible fixed assets	Obtain a list of assets scheduled for verification in year & confirm whether this has been undertaken as planned.	Review the documentation of the latest physical verification/reconciliation exercise for fixed assets. Confirm that positive confirmation was received from all relevant managers, and that discrepancies raised have been resolved and the general ledger updated.
Controls in relation to accuracy of depreciation, eg. reconciliation of movement in depreciation from prior year to movement in fixed asset balance. (DCC only)	Discuss with management how often the depreciation charge is reviewed and the process for investigating variances and documentation of review. For one review ensure it has been completed in line with management assertions.	Select a sample of monthly reviews, in line with sample sizes as set out on page 6, from the audited year, and obtain evidence that depreciation review has been completed on a timely basis and evidenced as reviewed..
Walkthroughs: Capital programme setting; Capital Expenditure; Reconciliation between the fixed asset register and the general ledger.		

Summary of controls to be tested (continued)

Control	Specific area of testing	Detailed testing requirements
Treasury management		
Monthly reconciliation of bank accounts and cash receipting system to the general ledger and cash book.	Discuss the process for reconciliations with management, including the process for investigating reconciling items and review. For one reconciliation ensure that this process has been followed.	For a sample in line with the sample sizes on page 6, confirm that reconciliations have been performed on a timely basis and evidenced as reviewed.
		Agree systems balances and significant reconciling items to supporting documentation and ensure reconciliation casts.
		Ensure all bank accounts with a significant balance and all frequently used bank accounts are considered.
Reconciliation of the cash receipting system to the general ledger (WC)	Re-perform a sample of reconciliations between the cash receipting system and the general ledger, obtaining explanations for any significant reconciling items.	Confirm that reconciliations have been produced in a timely fashion and have been evidenced as prepared and reviewed. Confirm that the reconciliation casts and any material reconciling items exist and agree to supporting documentation
Reconciliation of investment/borrowing records to the general ledger	Discuss the process for reconciliations with management, including the process for investigating reconciling items and review. For one reconciliation ensure that this process has been followed.	For a sample in line with the sample sizes on page 6, confirm that reconciliations have been performed on a timely basis and evidenced as reviewed.
		Agree systems balances and significant reconciling items to supporting documentation and ensure reconciliation casts.
		Confirm for a sample of short term investments and short term loans that the dates on which interest is payable and receivable are correctly flagged on the treasury management system
Walkthroughs: None		

Summary of controls to be tested (continued)

Control	Specific area of testing	Detailed testing requirements
Collection of local taxes (WPBC, WDCC and WC only)		
Periodic reconciliation of Council Tax and NNDR systems to the general ledger	Discuss the reconciliation process with management, including the follow up of reconciling items and review process. For one reconciliation ensure that it has been completed and reviewed in line with management's assertions.	For a sample in line with the sample sizes on page 6, confirm that reconciliations have been performed on a timely basis and evidenced as reviewed. Ensure that reconciling items are supported by evidence and the reconciliation casts.
Periodic reconciliation of the Council Tax and NNDR systems to the cash receipting system.	Discuss the reconciliation process with management, including the follow up of reconciling items and review process. For one reconciliation ensure that it has been completed and reviewed in line with management's assertions.	For a sample in line with the sample sizes on page 6, confirm that reconciliations have been performed on a timely basis and evidenced as reviewed. Ensure that reconciling items are supported by evidence and the reconciliation casts.
Periodic reconciliation of Council Tax and NNDR systems to the Valuation Office listing.	Discuss the reconciliation process with management, including the follow up of reconciling items and review process. For one reconciliation ensure that it has been completed and reviewed in line with management's assertions.	For a sample in line with the sample sizes on page 6, confirm that reconciliations have been performed on a timely basis and evidenced as reviewed. Ensure that reconciling items are supported by evidence and the reconciliation casts.
Independent review of exceptions: e.g. banding changes; suppressed accounts; overpayments and refunds.	Confirm that independent exception reviews of the Council Tax and NNDR systems are routinely performed. For one reconciliation ensure that it has been completed and reviewed in line with management's assertions.	For a sample of exception reports confirm that they have been produced and reviewed in accordance with the Authority's timetable throughout the financial year. For a sample of exceptions requiring review, confirm that evidence of this review exists.
Amendments to standing data require appropriate authorisation.	Confirm that changes to NNDR standing data are appropriate and authorised.	Obtain confirmation of annual rise in NNDR rate.
		Confirm that the increases have been accurately input and authorised.
	Confirm that changes to council tax standing data are appropriate and authorised.	Obtain minutes of Executive meetings to confirm the annual council tax Band D increase.
		Confirm that the Band D increase and other changes to standing data have been accurately input and authorised.

Summary of controls to be tested (continued)

Control	Specific area of testing	Detailed testing requirements
Periodic production and independent review of Council Tax and NNDR arrears and credit reports.	Ensure that Council Tax and NNDR arrears reports are produced routinely.	Confirm that a sample of arrears reports, based on the sample sizes on page 6, have been independently reviewed throughout the year with appropriate action taken.
Walkthroughs: Confirm that a sample of arrears reports have been independently reviewed throughout the year with appropriate action		
General ledger & financial accounting		
Access to the ledger and other IT systems is controlled and monitored	Confirm that appropriate password and access controls exist over the ledger and other IT systems	Obtain a list of all individuals with ledger / system access. For a sample of officers known to have recently left the audited body, confirm that these individuals no longer have access or profiles set up on the system.
		From the list of employees with ledger access, select a sample of employees and confirm that: - Each is an individual current employee of the audited body -Their system access is the minimum necessary to perform their role e.g. debtors clerks have access only to debtors ledger etc - Their ledger access and changes to it are supported by authorisation from their line manager or HR
	Exception reports are produced on a regular basis to monitor ledger use, for example to identify inactive user profiles, or ledger use at an unusual time or of an unusual nature	Document the range and frequency of exception reports produced.
		Test a sample of reports to confirm they were produced, reviewed and evidence of action taken documented.
Budgetary control: Management review of revenue income and expenditure against budget	Review budgetary control information produced to ensure that income and expenditure variances against budget are identified, reported and robustly investigated.	Select a sample of reports of income and expenditure against budget and check that they were produced for each month, and that the information contained is consistent with the general ledger.
		For sampled months, identify all material variances and obtain evidence from management accountants to confirm that the variance has been robustly investigated and explanations documented.

Summary of controls to be tested (continued)

Control	Specific area of testing	Detailed testing requirements
Journal entries to the general ledger are appropriately controlled	All journal entries are appropriately documented and reviewed by a second officer	From general ledger records, obtain a sample of journal transactions posted by a sample of different officers. For each journal, confirm that: - The accounting logic of the journal is appropriate; - The value of debits and credits posted is confirmed by supporting evidence; - An audit trail of who, when and why the journal was posted is retained; and - The journal has been reviewed by an appropriate second officer, and evidence of this documented. -Consider using appropriate sampling software to determine any journals posted at a weekend, ending in 999 and duplicated entries
	The ledger software will not allow one sided or unbalanced journal entries to be made.	Witness a member of staff trying to post a one-sided journal and an unbalanced journal.
Feeder systems are reconciled with the general ledger	Confirm that all material feeder system reconciliations are properly carried out	Obtain a listing of ledger codes. Identify all those codes which receive material transactions from a feeder system or sub-ledger. In each case, confirm that a reconciliation process exists to confirm the accurate transfer of data between the ledger and feeder system, and document the frequency of this.
		For each reconciliation identified, confirm that a sample of reconciliations have been performed with the frequency and timeliness expected during the year to date.
		For each reconciliation tested, re-perform in detail, including: - Agreeing balances to the ledger and feeder system; - Obtaining support for the validity of reconciling items; - Confirming that the reconciliation was reviewed by a second officer and that this was documented.

Summary of controls to be tested (continued)

Control	Specific area of testing	Detailed testing requirements
Suspense accounts are robustly reviewed and reconciled	All suspense accounts are reconciled on a regular basis, and action taken to ensure they do not contain material balances, supported by evidenced management review	Obtain a list of all suspense codes on the ledger. Ensure that each is reconciled on a regular basis and that no material items remain (either on a gross or net basis).
Closing balances from the prior year are accurately rolled forward to current year opening balances	Confirm that all current year opening balances are consistent to the closing balances reported in the audited prior year statutory accounts.	Obtain a ledger report of all opening balances (or trial balance as at 1 April 2011). Annotate all balances, including zero balances, to confirm that they agree to the closing balances in the prior year audited accounts.
Period and year end closedown processes are robustly controlled	Confirm that monthly and year end closure of the ledger is performed on a timely basis	For a sample of months, confirm that the ledger was closed and that no further accounting entries were made after period end financial reporting procedures were carried out.

Summary of controls to be tested (General IT Controls)

This section of the appendix reflects the complete set of General IT Controls from which KPMG select those appropriate to test on an annual basis, to support our reliance upon automated controls within the in-scope IT applications. Sample sizes for testing of General IT Controls should meet or exceed the minimum levels on page 6.

Recently, we have not sought to rely on General IT Controls in respect of Dorset Fire and Dorset Police, as we have undertaken alternative procedures for efficiency. However, our view on this may change over time.

Control	Specific area of testing	Detailed testing requirements
Access to Programs and Data		
The entity has a comprehensive IT security policy in place which is regularly reviewed (and updated where necessary) by appropriate IT management and is brought to the attention of all relevant staff	Through enquiry with relevant management and inspection of documents, determine whether: - IT Security Policy documentation is in place, with coverage of expected aspects of the IT environment relevant to financial reporting - a process is in place to ensure periodic review, update and approval of documentation by management - a process is in place to ensure users (including relevant third parties) are made aware of security requirements	For a sample of new joiners, inspect evidence of sign-up to security awareness and agreement to comply with security requirements. e.g. signed policy acceptance statement, security awareness training records
Data centres hosting production server environments for in-scope IT applications are secured from damage and unauthorised use	Through enquiry and observation, determine whether servers related to the systems in-scope are adequately physically protected from hazards, accidental and malicious damage, and environmental conditions. Through enquiry and observation of relevant documentation, determine whether procedures and controls exist to restrict access to data centres to appropriate personnel (including visitors, temporary staff, contractors and other third parties) and that access to data centres is reviewed on a periodic basis.	For a sample of new joiners with access to data centres, inspect evidence that appropriate request and authorisation was provided prior to access being granted. For a sample of leavers, confirm that access to data centres has been revoked in a timely manner. If required, where access for staff leavers has not been revoked, inspect the data centre access logs to identify where any access with leavers credentials may have occurred.

Summary of controls to be tested (General IT Controls)

Control	Specific area of testing	Detailed testing requirements
Access to Programs and Data		
Access within each in-scope IT application is controlled via the assignment of user roles, groups, profiles, etc. which enforces the segregation of duties set out in financial procedures and is appropriately documented	Through enquiry and observation, determine the method used in each in-scope IT application for restricting user access. Determine whether adequate controls are implemented to identify and monitor and resolve potential segregation of duties conflicts.	On an appropriate sample basis, determine whether controls related to segregation of duties have been operated as designed during the period. *Note: if segregation of duties is not enforced due to resource limitations, evaluate mitigating or compensating controls, e.g. periodic review of user activity where SoD conflicts are known.*
Evidenced, independent review of user access rights to in-scope IT applications is performed on an appropriately regular basis	Through enquiry and inspection of documentation, determine whether adequate procedures are in place to ensure user access rights are reviewed and subsequently updated on a periodic and regular basis. Inspect whether IT users' access rights are defined in a security policy or authorised access matrix.	For a sample of access reviews performed during the period, inspect evidence that reviews have been carried out in a timely manner and by appropriately knowledgeable members of staff. Determine whether these reviews have been formally documented and resulting actions and access amendments have been completed.
For each in-scope IT application, appropriate approvals are given for assignment of new/amended access	Through enquiry and inspection of documentation, determine whether adequate procedures are in place to establish user access, and whether management procedures require formal approval by appropriate line management for the establishment of users and granting of access rights. Where possible, perform a walkthrough of an example user addition and a user access amendment to ensure controls are in place as described.	For a sample of new user access and existing user access amendment (population produced via system-generated method directly from each in-scope IT application where possible), inspect evidence that access was granted subject to appropriate request and authorisation. For the sample selected, agree that the access approved and allocated as per each request has been assigned as such to the relevant user account.

Summary of controls to be tested (General IT Controls)

Control	Specific area of testing	Detailed testing requirements
Access to Programs and Data		
For each in-scope IT application, revocation of user access where required is performed in a timely manner	Through enquiry and inspection of relevant documentation, determine whether adequate procedures are in place to ensure that user access is revoked in a timely manner from in-scope IT applications where required. Review whether these procedures include all members of staff e.g. permanent (full-time and part-time), temporary, contracted, etc. Where possible, perform a walkthrough of an example user access revocation and ensure controls are in place as described.	Obtain from HR a listing of employees that have left. Obtain a listing of all active user accounts (system-generated directly from each in-scope IT application where possible). Reconcile the leavers listing with the active system accounts to validate that access has been revoked for all employees that have left. Where access has been retained, inspect system access logs to determine whether last use of user account exceeds related staff member's leaving date and investigate discrepancies.
		Obtain from HR a listing of employees that have transferred internally, where use of an in-scope IT application is reduced or no longer required. For a sample of these staff, determine whether access has been amended to reflect their new position, including appropriate documentation of request and authorisation for amendments in access to be made.
Adequate authentication methods and password-based access restrictions are enforced within each in-scope IT application	Through enquiry and inspection ,determine whether adequate methods and controls are in place for user authentication to in-scope IT applications. Inspect security standards to validate that password configuration settings are defined, e.g. min length, complexity, max duration, invalid login attempts threshold Through enquiry and inspection determine the procedures implemented to allow passwords to be reset in the event of loss or lockout. Walkthrough the procedure for one user to ensure controls are in place as described.	Determine whether password settings are applied globally to all users or if exceptions exist e.g. different for certain groups of users. For each applicable set of password settings, inspect the password configurations in place for each in-scope IT application (e.g. through system generated report or screen print) and determine if adequate and in line with defined policies.

Summary of controls to be tested (General IT Controls)

Control	Specific area of testing	Detailed testing requirements
Access to Programs and Data		
All applications have individual user ID's for business users as well as IT users. In case shared or system accounts exist, compensating controls are in place where needed	Through enquiry and inspection of policies and procedures, determine if appropriate standards for allocation of user ID's are in place. Determine how controls are implemented to restrict the use of any generic, shared and temporary user accounts. If any are identified, determine whether adequate procedures are in place to monitor their use.	Obtain a listing of all active user accounts (system-generated directly from each in-scope IT application where possible) and inspect for uniqueness and user naming conventions applied. Query the user ID listings to identify whether each individual user possesses only one user account and, for any discrepancies identified, inquire further for adequate reasons. Inspect the listing of user accounts to confirm that any generic, shared or temporary user IDs have been established according to policy. Validate that any unused standard / default system accounts have been locked or their password has been changed from default and secured.
Access to perform system administration duties within each in-scope IT application (e.g. user administration, changes to configuration, changes to password policies, etc.) and direct access to the underlying database is restricted only to appropriate individuals, use of this powerful access is governed by a suitable policy and monitored where deemed appropriate	Through enquiry and inspection of documentation, determine whether adequate procedures are in place to control: - the allocation of powerful application level accounts, how these are restricted, who is supposed to have access and who should approve such access privileges. - direct data access (e.g. SQL utilities, ODBC tools), access requirements (passwords and specific access restrictions) and logging/audit trails to track the usage of these facilities. *Note: Powerful and system level functions and accounts can include access via standard super user accounts, or access to sensitive transactions, functions or profiles.* Where monitoring procedures are in place, determine adequacy of scope, review and documentation (e.g. specific user activity, access to sensitive data, etc.) in line with allocation of powerful access.	Obtain listings of all user accounts (system-generated directly from each in-scope IT application where possible) with powerful or sensitive access, access to system level functions, or access to perform direct data maintenance. *Note: Where possible, include those user accounts that have had this level of access assigned temporarily during the period under audit.* Validate the appropriateness of these powerful access through discussions with management, comparison to organisational charts / authorised forms, Where monitoring procedures are in place, inspect sample of any formal documentation retained and assess whether performed in line with stated procedures.

Summary of controls to be tested (General IT Controls)

Control	Specific area of testing	Detailed testing requirements
Program Changes		
Business or IT requests for program change are logged and tracked through an appropriate method of documentation, approval and tracking and follow formal change management processes that enforces the use of change controls Program changes requested are prioritised for business criticality, assessed for potential impact to the business, and approved prior to development	Inquire of change management staff and inspect relevant documentation to confirm whether the organisation has a formally documented and approved change management process applicable to in-scope IT applications. Inquire of change management staff and inspect relevant documentation to confirm that all changes are tracked, prioritised, assessed and approved by an appropriate level of management prior to development. Conduct a walkthrough for one program change made to an in-scope IT application to determine whether controls are in place as described.	Obtain a listing of all program changes made during the period (system generated where possible). For a sample of program changes, inspect evidence that: - each change has been appropriately logged and documented, including assessment of business impact and priority - each change has been approved by appropriate management prior to development
Program changes are subject to formal testing by both IT personnel as Business. Test requirements are predefined and level of testing required is risk based. Test results are signed-off if the requirements have been met sufficiently. Separate test environments are used where appropriate	Inquire of change management staff and inspect relevant documentation to confirm the existence of a formal test strategy and methodology to test program changes. Validate that this includes appropriate specification of roles and responsibilities, types of tests required, detailed test requirements, requirements regarding test environments, approvals on test results from both business and IT, etc. Conduct a walkthrough for one program change to determine whether controls are in place as described.	For the sample of program changes already selected, inspect evidence that these have been tested and documented as required by the test strategy and procedures

Summary of controls to be tested (General IT Controls)

Control	Specific area of testing	Detailed testing requirements
Program Changes		
Program changes are formally approved before migration to production environment	Enquire of change / release management staff and inspect relevant documentation to confirm program changes are explicitly approved before release to production Conduct a walkthrough for one program change to determine whether controls are in place as described.	For the sample of program changes already selected, inspect evidence that these were appropriately approved before being released for migration to the production environment.
Implementing a program change into the production environment of an in-scope IT application is limited to specific change management personnel that had no involvement in the development of the change	Through enquiry and observation, validate that adequate segregation of duties exists in the change control process that enforces appropriate segregation between requesting, developing, testing and implementing program changes where possible. Determine whether change release access to the in-scope IT application's production environment is limited to change management personnel. Conduct a walkthrough for one program change to determine whether controls are in place as described.	For the sample of program changes already selected, inspect evidence that segregation of duties was enforced throughout the change process, including segregation between requesting, developing, testing and implementing changes where possible. *Note: if segregation of duties is not possible due to resource limitations, evaluate other mitigating controls in place, e.g. periodic independent review of changes migrated to production*
Separate environments exist between development, test and production, with developers having no or restricted access within the production environment	Through enquiry and observation, validate that separate environments exist for development, test and production. Determine whether policies exist to appropriately restrict developer access to the production environment.	Obtain evidence of the existence of separated environments for (at least) development, test and production (e.g. Screen print, system generated report, etc.) Obtain listings of developer access to the environments identified and review these for appropriate segregation. *Note: if restriction of developer access to production is not possible due to resource limitations, evaluate other mitigating controls, e.g. logging, monitoring and review of developer activity in production.*

Summary of controls to be tested (General IT Controls)

Control	Specific area of testing	Detailed testing requirements
Program Changes		
Changes to the 'configuration' of in-scope IT applications (i.e. changes to configurable parameters within the application) are documented and are subjected to an appropriate methodology that includes documenting, testing, and approving changes	Inquire of change management staff and inspect relevant documentation to confirm whether the organisation has a formally documented and approved process for making configuration changes to in-scope IT applications. Inquire of change management staff and inspect relevant documentation to confirm that all configuration changes are documented, tested and approved prior to implementation. Conduct a walkthrough for one configuration change to determine whether controls are in place as described.	Obtain a listing of all configuration changes made during the period (system generated where possible). For a sample of configuration changes, inspect evidence that: - each change has been appropriately logged and documented - each change has been tested prior to implementation in production - each change has been approved prior to implementation in production *Note: if process does not differ from that followed for standard program changes, testing could be performed across the full population of standard and configuration changes*
Emergency changes (i.e. changes that are urgent and therefore require to be fast-tracked for implementation outside of normal program or configuration change procedures) are appropriately approved before implementing to production	Inquire of change management staff and inspect relevant documentation to confirm whether the organisation has a formally documented and approved process for making emergency changes to in-scope IT applications. Inquire of change management staff and inspect relevant documentation to confirm that all emergency changes are subject to the key controls that apply for regular changes (tracked, approved, tested, test signed-off, migrated, etc), whether retrospectively or in advance. Conduct a walkthrough for one emergency change to determine whether controls are in place as described.	Obtain a listing of all emergency changes made during the period (system generated where possible). For a sample of emergency changes, inspect evidence that emergency change procedures have been adhered to, and key controls that apply for regular changes are implemented effectively (tracked, approved, tested, test signed-off, migrated, etc) in retrospect where applicable.

Summary of controls to be tested (General IT Controls)

Control	Specific area of testing	Detailed testing requirements
Program Development (if applicable – to be determined by KPMG in audit scoping and planning)		
IT Projects (including new acquisition and major developments of existing in-scope IT applications) are logged and tracked through an appropriate documentation, approval and tracking tool and follow company policy and processes that enforces the use of controls regarding prioritisation, funding, testing and approving	Enquire of relevant staff and inspect documentation to confirm whether the organisation has a formally documented and approved Software Development Life Cycle (SDLC) process applicable to relevant in-scope IT applications. Inquire of relevant staff and inspect documentation to confirm whether the organisation has a formally documented and approved Program and/or Project Management process applicable to relevant IT projects.	Inspect evidence to validate that relevant IT projects have followed the applicable SDLC and Project Management processes. Ensure that these projects have progressed through appropriate stage-gate controls during key project phases, such as definition, prioritisation, approval, design, development, testing and implementation
IT Projects (including new acquisition and major developments of existing in-scope IT applications) are subject to formal testing by both IT personnel and relevant business personnel. Test requirements are predefined and level of testing required is risk based. Test results are signed-off if the requirements have been met sufficiently before go-live	Inquire of relevant staff and inspect documentation to confirm the existence of a formal test strategy and methodology to be used for acquisition and major development projects. Validate that this includes appropriate specification of roles and responsibilities, types of tests required, detailed test requirements, requirements regarding test environments, approvals on test results from both business and IT, etc.	For relevant IT projects, verify that adequate test scripts, go-live criteria, and test results are available as required by the test strategy and procedures and have been signed-off as such by appropriate level of management.
Migration of data follows appropriate data migration processes that enforces the use of strict controls to ensure data integrity during and after migrations	Enquire of relevant staff and inspect documentation to confirm whether the organisation has a formally documented and approved data migration process applicable to relevant IT projects. Validate that this includes requirements for sufficient design, testing and sign-off of data migration.	Inspect evidence to validate that relevant IT projects have followed the applicable data migration process. Verify that testing has been performed with sufficient detail, and any exceptions found were corrected where appropriate. Verify that data migration has been signed-off by an appropriate level of business and IT management.

Summary of controls to be tested (General IT Controls)

Control	Specific area of testing	Detailed testing requirements
Computer Operations (if applicable – to be determined by KPMG in audit scoping and planning)		
Appropriate backup polices and procedures are followed to ensure timely backups are made of in-scope IT applications and data, and appropriate availability and retention of backup tapes is ensured	Enquire of IT Operations staff and inspect relevant documentation to confirm whether the organisation has a formally documented and approved backup process applicable to in-scope IT applications. Inquire of relevant staff and inspect documentation to assess whether in-scope IT applications and data are being included in the backup process.	Obtain evidence of backup log files to validate that a sample of backups for in-scope IT applications were completed successfully. If failures are noted, ensure these have been captured as incidents and are subject to relevant Incident Management controls that ensure eventual completion of the backup.
Appropriate system restoration polices and procedures are followed to ensure in-scope IT applications and data can be restored successfully after an incident, and that system recovery procedures are tested periodically.	Inquire of IT Operations staff and inspect relevant documentation to confirm whether the organisation has a formally documented and approved system restoration process applicable to in-scope IT applications. Determine whether system recovery procedures are tested at least annually to ensure recovery success in the event of a major incident that would require this.	Obtain a schedule of system / data restoration tests performed and validate completeness by ensuring all in-scope IT applications have been subject to a restoration test during the stated period. For a sample of restoration tests, inspect evidence to confirm that restoration procedures were performed according to the defined procedure and test results were signed-off by an appropriate level of management. Validate that relevant documentation has been appropriately amended, where necessary, following restoration tests.
Appropriate incident and problem management processes are in place to capture incidents and failures relating to in-scope IT applications, to prioritise for business criticality, and to ensure these are tracked through an appropriate resolution. Formal incident response procedure and escalation procedures are developed and implemented.	Inquire of IT Operations staff and inspect relevant documentation to confirm whether the organisation has a formally documented and approved Incident and Problem Management process. Determine whether Problem and Incident Management governance exists through the reporting and monitoring of KPIs, SLAs and problem trends. Observe a walkthrough of the Problem and Incident Management process to determine all requirements are met.	For a sample of incidents deemed to be high / urgent priority, inspect evidence to validate that: - the tickets had been assigned the appropriate priority and incident resolution team - the processes followed to resolve the issue were reasonable and done on a timely basis based on assigned priority/defined SLAs Inspect a sample of Problem and Incident management monitoring reports/dashboards to validate that the monitoring and governance process was adequately performed.

Summary of controls to be tested (General IT Controls)

Control	Specific area of testing	Detailed testing requirements
Computer Operations (if applicable – to be determined by KPMG in audit scoping and planning)		
Appropriate job monitoring processes are followed to monitor key system jobs and interfaces to ensure completeness and timeliness of system and data processing, and to identify any interruptions in time for follow-up and resolution	Enquire of IT Operations staff and inspect relevant documentation to confirm whether the organisation has a formally documented and approved job monitoring process applicable to in-scope IT applications. Observe a walkthrough of the job monitoring process to determine all requirements are met.	Obtain a list of relevant system/scheduled jobs. For a sample of jobs, inspect evidence that jobs are being controlled in line with the job monitoring requirements. Verify that errors in job processing have been captured as incidents and are subject to Incident Management controls that ensure eventual completion of the job processing. *Note: testing of changes to scheduled jobs should be covered in Program Change and Access to Programs and Data, unless specific processes exist for batch / scheduled jobs.*

Summary of controls to be tested (IT Controls) (continued)

Scope of system affecting opinion
With regards to general IT controls, the following systems are within scope for external audit for the 12/13 audit year:
SAP (AP, AR, GL) (DCC and WC)
Academy, Sage, Northgate (WPBC and WDDC)
Simdell and new housing system (WC)
Civica Icon (WC)
Northgate – Revenue & Benefits system
Agresso- Dorset Police – System changeover

cutting through complexity™